



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/577,224	05/23/2000	Lundy Lewis	019287-0317296	4214
909 7590 02/09/2009 PILLSBURY WINTHROP SHAW PITTMAN, LLP P.O. BOX 10500 MCLEAN, VA 22102				
EXAMINER				
ENGLAND, DAVID E				
ART UNIT		PAPER NUMBER		
2443				
MAIL DATE		DELIVERY MODE		
02/09/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte LUNDY LEWIS

Appeal 2008-3109
Application 09/577,224¹
Technology Center 2100

Decided:² February 9, 2009

Before JOHN C. MARTIN, LANCE LEONARD BARRY, and
JEAN R. HOMERE, *Administrative Patent Judges*.

MARTIN, *Administrative Patent Judge*.

DECISION ON APPEAL

¹ Filed September 10, 1999.

² The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1, 3-6, and 23-27, which are all of the pending claims.

Oral argument was held on January 22, 2008.³

We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

A. Appellant's invention

Appellant's invention is directed to various aspects of service level management (SLM), whereby an entity (such as a company, university, Internet service provider (ISP), electronic commerce (EC) provider, etc.) may, for example, map components of a network (i.e., network devices, transmission media, computer systems, and applications) into services in order to assess the state of those services. Specification 1:29 to 2:3. The state of those services, referred to as service parameters, may include availability, response time, security, and integrity. *Id.* at 2:3-5.

Appellant's Figure 18 is reproduced below.

³ The record includes a transcript of the hearing.

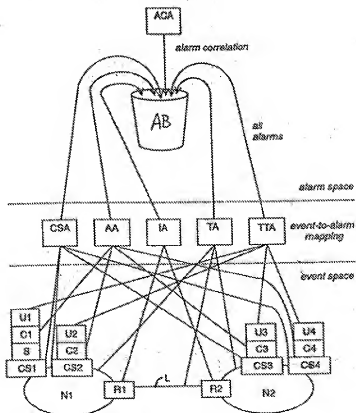


Figure 5.8 *Fig. 18*

Figure 18 shows an embodiment of a simplified enterprise network including monitoring agents and an alarm correlation bucket. *Id.* at 16:24-27.

Two networks N1 and N2 are connected by a communications link L. *Id.* at 47:7-8. A first router R1 associated with network N1 communicates with a second router R2 associated with network N2 through the communications link L. *Id.* at 47:8-10. The two networks, and their respective systems, are together referred to as the enterprise. *Id.* at 47:10-11. Two computer

systems CS1, CS2, reside on network N1 and two computer systems CS3, CS4 reside on network N2. *Id.* at 47:11-12. As an explanatory example, a client/server application (e.g., a database application) that is supported by the network infrastructure and the computer systems is present. *Id.* at 47:12-14. Specifically, a database server S resides on computer system CS1 and database clients C1-C4 reside on computer systems CS1-CS4, respectively. *Id.* at 47:14-16. The four client applications are Graphical User Interface (GUI) interfaces through which users U 1-U4, respectively, interact with database server S. *Id.* at 47:16-17.

A network infrastructure agent IA monitors the operation of routers R1, R2; a computer system agent CSA monitors the operations of computer systems CS1-CS4; an applications agent AA monitors database server S and the operation of database clients C1-C4; a traffic agent TA monitors network traffic that flows over networks N1, N2 and over the communications link L; and a trouble-ticketing system agent TTA monitors users U1-U4 who depend on the client/server database application. *Id.* at 47:18-23. The users log problems in the trouble-ticketing system agent when their database transactions are not operating properly. *Id.* at 47:23-24.

Each of the five agents (CSA, AA, IA, TA, TTA) monitors its respective portion or aspect of the operation of the enterprise by detecting “events.” *Id.* at 47:25-26. When an event is detected by any of the agents, a report of this event may be output by the respective agent. *Id.* at 47:26-27.

For example, if users U3 and U4 report an unacceptably slow behavior of their database transactions, there may be trouble-tickets logged with the trouble-ticketing system agent TTA. *Id.* at 47:28-29.

Each monitoring agent processes or sifts through its respective detected events and makes a determination about whether or not to issue an alarm with respect to its area of its interest in the enterprise's operation. *Id.* at 48:9-11. The issued alarms are sent to the alarm bucket AB for correlation with other alarms by an alarm correlation agent ACA. *Id.* at 48:11-13.

Referring to the flow chart depicted in Figures 19 and 20, the Specification more particularly explains that in the alarm bucket, represented as step 162,

[t]he alarms are correlated and evaluated to determine the network operation status, step 163. Optionally, the network operation status may be reported to a network administrator, step 164. . . . In step 165, corrective actions that are necessary for operating the network at a desired level of operation[] are identified. In step 166, the corrective actions may be implemented, or the proposed corrective actions reported to the network administrator.

Id. at 48:19-25. Of those steps, Appellant reads the step of “transmitting the correlated alarms to an enterprise management system to analyze, across a network, causes of the correlated alarms,” recited in claim 1 (reproduced below), on step 165. Br. 3.

B. The claims

The independent claims before us are claims 1, 23, and 27, of which claim 1 reads:

1. A method for managing network services associated with a service level management domain to provide service level management, the method comprising the steps of:

monitoring, by a plurality of monitoring agents, operational characteristics of a network service associated with a service level management domain and supporting one or more business processes under service level management, each monitoring agent detecting events of a select type of the associated operational characteristics from the network service and mapping such events into alarms;

transmitting the alarms from the plurality of monitoring agents to an alarm correlation agent, which analyzes the alarms to produce correlated alarms; and

transmitting the correlated alarms to an enterprise management system to analyze, across a network, causes of the correlated alarms;

whereby the alarms and the correlated alarms are indicative of a degradation in service level or potential degradation in service level.

C. The references and rejection

The Examiner relies on the following references:

Maccabee et al. (Maccabee)	US 6,108,700	Aug. 22, 2000 (filed Aug. 1, 1997)
----------------------------	--------------	---------------------------------------

Appeal 2008-3109
Application 09/577,224

Koperda et al. (Koperda)	US 6,230,203 B1 May 8, 2001 (filed Mar. 14, 1997)
Bhoj et al. (Bhoj)	US 6,304,892 B1 Oct. 16, 2001 (filed Nov. 2, 1998)
Medhat et al. (Medhat)	US 6,314,103 B1 Nov. 6, 2001 (filed Feb. 20, 1998)
Roytman et al. (Roytman)	US 6,356,282 B2 Mar. 12, 2002 (filed Dec. 4, 1998)

Claims 1, 23, 24, 26, and 27 stand rejected under 35 U.S.C. § 103(a) for obviousness over Maccabee in view of Roytman and Medhat.

Claims 3-6 stand rejected under 35 U.S.C. § 103(a) for obviousness over Maccabee in view of Roytman, Medhat, and Koperda.

Claim 25 stands rejected under 35 U.S.C. § 103(a) for obviousness over Maccabee in view of Roytman, Medhat, and Bhoj.

Appellant argues the merits of only the independent claims, i.e., claims 1, 23, and 27.

THE ISSUES

Generally speaking, the issue is whether Appellant has shown reversible error by the Examiner in maintaining the rejection. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) (“On appeal to the Board, an applicant can overcome a rejection by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.”) (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

The principal issue regarding the rejection of claim 1 is whether Appellant has shown that the Examiner erred in reading the recited “monitoring agents” on Maccabee’s sensors 200, reading the recited “events” on the changes in state monitored by those sensors, reading the recited “alarms” on the “events” generated by those sensors, and reading the recited “correlated alarms” on Maccabee’s “transactions.”

The principal issue regarding the rejection of claims 23 and 27 is whether Appellant has shown that the Examiner erred in reading the recited “a value in the range of values, the value being a performance index of the grade of the service” on Roytman’s alarm severity levels, which include “critical,” “major,” “warning,” “minor,” “normal,” and “indeterminate.” Roytman, col. 7, ll. 58-61.

PRINCIPLES OF LAW

Application claims are interpreted as broadly as is reasonable and consistent with the specification, *In re Thrift*, 298 F.3d 1357, 1364 (Fed. Cir. 2002), while “taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in the applicant's specification.” *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997).

“[T]he examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability.” *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). A rejection under 35 U.S.C. § 103(a) must be based on the following factual determinations: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) any objective indicia of non-obviousness. *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966)).

“The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *Leapfrog Enter., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161 (Fed. Cir. 2007) (quoting *KSR Int’l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1739 (2007)). Discussing the obviousness of claimed combinations of elements of prior art, *KSR* explains:

When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. *Sakraidia* [v. *AG Pro, Inc.*, 425 U.S. 273 (1976)] and *Anderson's-Black Rock, Inc. v. Pavement Salvage Co.*, 396 U.S. 57 (1969)] are illustrative—a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions.

KSR, 127 S. Ct. at 1740. If the claimed subject matter “involve[s] more than the simple substitution of one known element for another or the mere application of a known technique to a piece of prior art ready for the improvement,” *id.*,

it will be necessary . . . to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.

Id. at 1740-41. “To facilitate review, this analysis should be made explicit.”

Id. at 1741. That is, “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *Id.* (quoting *Kahn*, 441 F.3d at 988).

ANALYSIS

A. Maccabee

Maccabee's invention is directed to an improved method and system for measuring and reporting availability and performance of end-to-end (ETE) business transactions. Maccabee, col. 3, ll. 14-23.

Maccabee's Figure 1C is reproduced below.

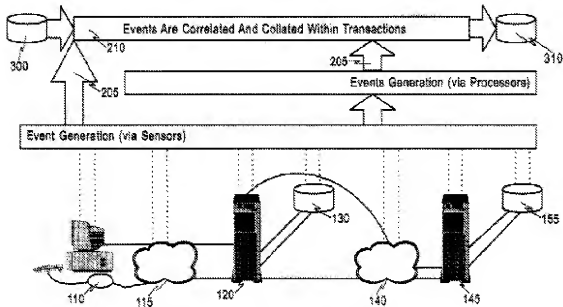


Fig. 1C

Figure 1C depicts an example of ETE (end-to-end) SLMS (Service Level Management System) Transaction Generation. *Id.*, col. 6, ll. 12-16.

Sensors (labeled 200 in Fig. 1B) interact with the software and hardware components through which the business transaction is processed, glean changes in state that result in the generation of "events" (205). *Id.*,

col. 7, ll. 39-42. If the change in state is such that an event can be generated, the sensor further checks control rules (Fig. 2), e.g., filters, to determine if it may generate the event. *Id.*, col. 7, ll. 51-54. When appropriate, the sensor generates an event that describes the change in state, when and where it has occurred, and any extra data necessary to uniquely identify the event. *Id.*, col. 7, ll. 54-57.

More particularly, an event contains identifying information such as a time-stamp and correlation data subsequently used by the system to associate the event with other events into transactions. *Id.*, col. 8, ll. 29-32. Transactions are collections of related or linked events and/or other transactions. *Id.*, col. 8, ll. 36-38. The event correlations (305) are based on common data attributes (correlation data) found within the events (205). *Id.*, col. 8, ll. 38-40. Events can be assessed to determine if the event should begin a new transaction, and/or if the event should be incorporated within an existing “work-in-progress” transaction. *Id.*, col. 8, ll. 40-43.

Figure 1D is similar to Figure 3 and additionally shows Report Generation (400), which involves the retrieval and manipulation of “transactions” to glean information relating to availability and performance of business transactions. *Id.*, col. 8, ll. 60-62. The report generation facilities enable transactions to be viewed (415) as graphical aggregates or in detailed decompositions showing the contribution of select stages of processing the business transaction has undergone. *Id.*, col. 9, ll. 5-9. An

example directed to a browser response time and decomposition is depicted in Figure 14 (*id.*, col. 9, ll. 9-10), reproduced below.

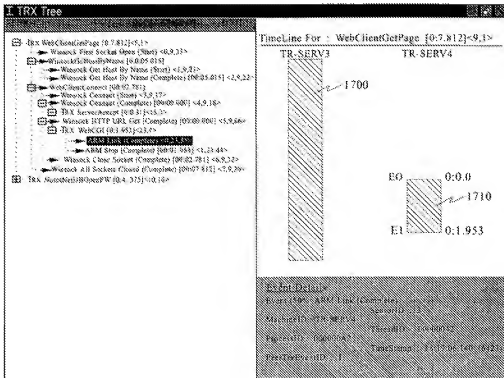


Fig. 14

The left part of Figure 14 describes Transaction Generation from the arriving events. *Id.*, col. 14, ll. 20-21. The right side of Figure 14 depicts duration-representative bars 1700 and 1710, of which left bar 1700 represents an approximation of total response time and right bar 1710 represents the server component of the total response time. *Id.*, col. 14, ll. 22-26. The network component of the response time can be derived by subtraction of bar 1710 from bar 1700. *Id.*, col. 14, ll. 26-28.

B. The rejection of claim 1

The Examiner reads the recited “monitoring agents” on Maccabee’s sensors 200, reads the recited “events” on the changes in state monitored by those sensors, reads the recited “alarms” on the “events” generated by those sensors, and reads the recited “correlated alarms” on Maccabee’s “transactions.” *See* Final Action 2-3, paras 5-6; Answer 3-4, 14-15. For example, the Examiner explains that “[Maccabee’s] ‘sensors’ [are] to also be interpreted as [the recited] ‘agents’” (Answer 4), thereby indicating that the changes in state sensed by those sensors correspond to the recited “events.” Furthermore, the Examiner reads the step of “transmitting the alarms from the plurality of monitoring agents to an alarm correlation agent, which analyzes the alarms to produce correlated alarms” on Maccabee’s disclosure of “any correlation data useful for later associating the event with the other events to form transactions” (*id.*), thereby indicating that the recited “alarms” read on Maccabee’s “events” 205 and that the recited “correlated alarms” read on Maccabee’s “transactions.” Regarding the meaning of “alarm,” the Examiner further stated in the Answer (at 14) that “[t]here is no teaching[] in the claims that would suggest that an alarm is anything else but a message as to what has happened in a network, either bad or good.”

Some of Appellant’s arguments regarding the rejection are unconvincing because they are based on a misunderstanding of the Examiner’s position. For example, rather than recognizing that the Examiner reads the recited “alarms” on Maccabee’s “events” and the recited

“correlated alarms” on Maccabee’s “transactions,” Appellant asserts that the Examiner “alleges that [Maccabee’s] ‘transactions’ are the same as [the recited] ‘alarms’” (Br. 7) and that in order to satisfy claim 1 “Maccabee would have to describe a system that analyzes the transactions to produce ‘correlated’ transactions.” *Id.*

Appellant also argues that “[Maccabee’s] ‘*transaction*’ represents a series of processing stages associated with a task, request, application, etc., whereas an ‘*alarm*’ is based on an operational characteristic of a network resource” (*id.*) (emphasis added), which argument is presumably based on the requirement of claim 1 that “each monitoring agent detect[] events of a select type of the associated operational characteristics from the network service and map[] such events into alarms.” This argument, too, is unconvincing because it incorrectly assumes that the Examiner is reading the recited “alarms” on Maccabee’s “transactions” rather than on Maccabee’s “events.”

Nor does the above-quoted “operational characteristics” claim language distinguish the recited “alarms” from Maccabee’s “events,” on which the Examiner reads the recited “alarms.” Maccabee’s “events” can accurately be described as based on “an operational characteristic of a network resource” because they are derived from changes in state in software and hardware components that are sensed by sensors 200 (the recited “monitoring agents”). Maccabee, col. 7, ll. 38-42.

The Brief (no reply brief was filed) makes no other argument that can reasonably be construed as an attempt to distinguish the recited “alarms” from Maccabee’s “events.” Although the Brief explains (at 3) that descriptive support for the recited “wherein” clause, which specifies that “the alarms and the correlated alarms are indicative of a degradation in service level or potential degradation in service level,” can be found at page 26, lines 11-15 of the Specification, the Brief does not even mention the “wherein” clause in the “Argument” portion of the Brief, let alone explain how that clause should be construed and why the language thus construed precludes the recited “alarms” from being read on Maccabee’s “events.” Furthermore, Appellant did not file a reply brief challenging the Examiner’s conclusion that “[t]here is no teaching[] in the claims that would suggest that an alarm is anything else but a message as to what has happened in a network, either bad or good.” Answer 14.

Counsel for Appellant argued during oral argument that the claim term “events” would have been understood to have a meaning that requires it to be read on Maccabee’s “events” and thus precludes the recited “events” from being read on the changes in state detected by Maccabee’s sensors 205. Hr’g Tr. 13:17 to 14:17. This argument does not appear in the Brief and is therefore entitled to no consideration in this appeal proceeding. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2007) (“Any arguments or authorities not included in the brief or a reply brief filed pursuant to § 41.41 will be refused consideration by the Board, unless good cause is shown.”).

Appellant also argues that Maccabee and Roytman, considered alone or in combination, fail to disclose or suggest “transmitting the correlated alarms to an enterprise management system *to analyze*, across a network, *causes* of the correlated alarms.” Br. 8 (emphasis added). We note that Appellant’s argument and the Examiner’s explanation of the rejection suggest a common belief that the “transmitting” step in question requires that the enterprise management system actually analyze or be used to analyze the causes of the correlated alarms. We do not agree. The only function required by this “transmitting” step is to “transmit[] the correlated alarms to an enterprise management system.” The language “to analyze, across a network, causes of the correlated alarms” is simply a statement of the intended use of the enterprise management system. Consequently, this claim language is either entitled to no weight or, at most, requires that the correlated alarms that are sent to the enterprise management system be *capable* of being used “to analyze, across a network, causes of the correlated alarms.” Appellant has not asserted, let alone demonstrated, that Maccabee’s transactions, on which the Examiner reads the recited “correlated alarms,” are incapable of being analyzed to identify the causes of the correlated alarms.

Furthermore, assuming for the sake of argument that the claim requires that the recited enterprise management system be used for analyzing the causes of the correlated alarms (Maccabee’s “transactions”), Appellant has not shown that the Examiner erred in finding such a teaching in the

combined teachings of Maccabee and Roytman. Although the Examiner initially relied for such a teaching on Roytman's disclosure in column 2, lines 34-51 of mapping alarms to corresponding nodes in a topology database (Final Action 3), the Examiner at page 17 of the Answer additionally relies on the listing of the "Example Web Commerce Transaction Definition" bridging columns 1 and 2 of Maccabee. Specifically, the Examiner explained that

[i]n Maccabee, column 14, lines 30 et seq., it is stated that the links between the events and transactions take place and that the T1, T2 and T3 are transactions or specific components that caused the event to happen as seen in T3, "ServerAccept" as once example. As can be seen in Figs. 11 - 14, with emphasis on figure 14, and the supporting text, Maccabee teaches the claimed language.

Answer 17. Appellant has not addressed this position of the Examiner, let alone demonstrated that it is erroneous. Furthermore, it would appear that the claimed function of identifying the cause of the correlated alarms (i.e., Maccabee's "transactions") is broad enough to read on duration bars 1700 and 1710 in Figure 14, which respectively represent the overall response time and the response time of the server and from which bars the network response time can be derived by subtraction. Maccabee, col. 14, ll. 20-26. Thus, in that example, analysis of the duration bars identifies the network as the primary cause of the overall delay.

As already noted, Appellant has not separately argued the "wherein" clause, which provides that "the alarms and the correlated alarms are

indicative of a degradation in service level or potential degradation in service level,” for which teaching the Examiner relies on Medhat. Answer 5.

In view of our conclusion that claim 1 does not require that the enterprise management system analyze, or be used to analyze, the causes of the correlated alarms, and further in view of our alternative finding that, even assuming the claim require such analysis, Appellant has failed to show reversible error in the Examiner’s finding that Maccabee (e.g., Fig. 14) contains such a teaching, we do not reach, at least with respect to claim 1, Appellant’s argument that the Examiner’s rationale for relying on Roytman for such a teaching is unpersuasive. Br. 11.

Because Appellant has failed to demonstrate any reversible error in the Examiner’s rejection of claim 1, we are affirming the rejection of that claim.

C. Analysis of the rejection of claims 23 and 27

Although the Examiner selected claim 27 when explaining the rejection of claims 23 and 27, we will begin our analysis with claim 23, which is the broader claim in several respects and reads as follows:

23. A method for monitoring a business process having at least one service associated with a service level management domain to provide service level management for an entity performing the business process, the service having a predefined state expressed as a range of values representing a grade of service, the method comprising the steps of:

collecting data on one or more resources of a network associated with the service level management domain, the network being capable of performing one or more functions to provide the entity with a service to allow the entity to perform the business process;

monitoring one or more parameters from the collected data, the one or more parameters providing an indication of an operational characteristic of the service provided by the network;

determining from the operational characteristic a value in the range of values, the value being a performance index of the grade of the service associated with the service level management domain; and

monitoring the value to provide service level management for the entity performing the business process.

The Examiner (Answer 6) reads the first and second steps (which are identical to the second and third steps of claim 27) on Maccabee's use of sensors 200 to generate "events" in response to changes in state of software and hardware components. Maccabee, col. 7, ll. 37-60. At page 6 of the Answer, the Examiner reads the third step (which is broader than the corresponding fourth step in claim 27) and presumably also the fourth step (which has no similar corresponding step in claim 27) on Roytman.

Roytman's invention provides an improvement of the display format provided by a conventional Solstice Enterprise Manager™ (Solstice EM) network management system (Roytman, col. 1, ll. 42-45; col. 47-49), which system is described in detail in columns 1-9. The Examiner relies on features of the conventional Solstice EM™ system.

Roytman's Figure 1 is reproduced below.

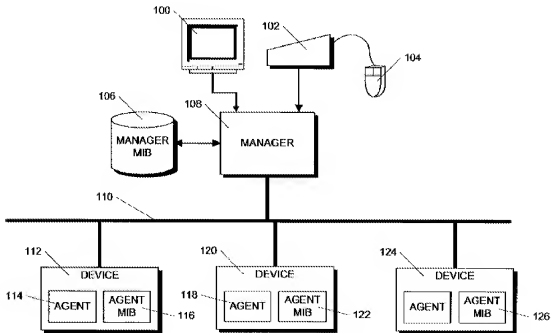


FIG. 1 (Prior Art)

Figure 1 is a block diagram of a distributed network management system on which Roytman's network management system can run. *Id.*, col. 4, ll. 30-33. Each device node 112, 120, and 124 corresponds to a managed device, such as a processor, printer, storage device, network adapter card or other network apparatus. *Id.*, col. 5, ll. 13-16. The state of each managed device is monitored and controlled by an agent program running in the node. *Id.*, col. 5, ll. 16-18.

In discussing Figure 5, which illustrates a portion of alarm log database 500 that is generated by the Solstice EMTM network and contains

alarm records 502 to 518 (*id.*, col. 6, l. 66 to col. 7, l. 1), Roytman explains that “alarm records 502-518 include information concerning the date (and time) of an alarm and the alarm source and may additionally include other information helpful to network management personnel in identifying the *cause* of the alarm and its solution.” *Id.*, col. 7, ll. 1-5 (emphasis added).

Figure 6 shows the conventional window 600 with a menu bar 602 that indicates several alarm attributes, including “perceived severity.” *Id.*, col. 7, ll. 54-56. The perceived severity is an attribute of each alarm, indicating the seriousness of the problem which caused the alarm. *Id.*, col. 7, ll. 56-58. Each alarm is assigned one of a predetermined number of severity levels, including “critical,” “major,” “warning,” “minor,” “normal,” and “indeterminate.” *Id.*, col. 7, ll. 58-61.

In the “association” viewing mode, such as that illustrated in Figure 6, an alarm listed in the table of alarms represents a group of similar alarms, with the alarm selected to represent the group being either the highest severity or the most recent. *Id.*, col. 8, ll. 11-15.

The Examiner (Answer 6, 18) reads the recited “range of values” on Roytman’s disclosure that each alarm is assigned one of a predetermined number of severity levels, including “critical,” “major,” “warning,” “minor,” “normal,” and “indeterminate.” *Id.*, col. 7, ll. 58-61. Appellant argues that “Roytman fails to teach or suggest ‘determining from the operational characteristic a value in the range of values,’ as recited in claims 23 and 27.”

Br. 10. However, Appellant does not explain why it is improper to read the recited “value in the range of values” on any of Roytman’s severity levels.

Appellant next more specifically argues:

Roytman displays the severity levels in a window for an operator to view (col. 7, lines 54-65), without “determining from the operational characteristic a value . . . being a performance index of the grade of the service associated with the service level management domain.” In other words, Roytman deals with the severity or characteristics of the alarm itself, not the relation between the alarm severity and “a performance index of the grade of the service.”

Br. 10. We do not agree. This argument appears to be based on the assumption that the recited “service” must comprise a plurality of monitored resources resulting in a plurality of alarms. However, the claim language “one or more resources,” “one or more functions,” and “one or more parameters” permits the recited “service” to consist of a single monitored device. Under these circumstances, the recited “performance index of the grade of the service” can be read on the severity level of an alarm that corresponds to a single monitored device.

As explained above, in our analysis of the rejection of claim 1 we found it unnecessary to reach Appellant’s arguments (Br. 11) against the Examiner’s rationale for combining the teachings of Maccabee and Roytman so as to satisfy the “to analyze, across a network, the causes of the correlated alarms” language of that claim. We find nothing in Appellant’s arguments against the combination of Maccabee and Roytman that specifically concerns the rejection of claims 23 and 27. Instead, the only claim language

addressed in those arguments is the above-quoted “cause” language of claim 1. Br. 11.

Because Appellant has not demonstrated reversible error in the Examiner’s rejection of claim 23, we are affirming the rejection of that claim and also the rejection of its unargued dependent claims 24 and 26, which stand rejected on the same ground as claim 23.

Regarding claim 27, Appellant makes the same arguments that were made with respect claim 23 and have been determined to be unpersuasive for the reasons given above. Accordingly, we are affirming the rejection of claim 27.

D. The rejection of dependent claims 3-6

The rejection of claims 3-6 for obviousness over Maccabee in view of Roytman, Medhat, and Koperda is affirmed because Appellant does not separately argue the merits of any of these claims, all of which depend on claim 1, whose rejection has been affirmed. *See In re Nielson*, 816 F.2d 1567, 1572 (Fed. Cir. 1987).

E. The rejection of dependent claim 25

The rejection of claim 25 for obviousness over Maccabee in view of Roytman, Medhat, and Bhoj is affirmed because this rejection is not separately argued and because claim 25 depends on claim 23, whose rejection has been affirmed.

DECISION

The rejection of claims 1, 23, 24, 26, and 27 under 35 U.S.C. § 103(a) for obviousness over Maccabee in view of Roytman and Medhat is affirmed.

The rejection of claims 3-6 under § 103(a) for obviousness over Maccabee in view of Roytman, Medhat, and Koperda is affirmed.

The rejection of claim 25 under § 103(a) for obviousness over Maccabee in view of Roytman, Medhat, and Bhoj is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. §§ 41.50(f) and 41.52(b).

AFFIRMED

msc

PILLSBURY WINTHROP SHAW PITTMAN, LLP
P.O. BOX 10500
MCLEAN, VA 22102